2. Закон України “Про інформацію” від 2 жовтня 1992 року // Відомості Верховної Ради України – 1992. – № 48. – Ст. 651.

3. Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки” // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

4. Закон України “Про основи національної безпеки України” // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351.

5. Гавловський В. Організаційно-правові питання формування державної інформаційної політики в Україні / В.Гавловський, В.Гриценко, В.Цимбалюк // Збірник наукових праць Академії державної податкової служби України. – 2002. – № 3 (17). – С. 177–182.

6. Петрик В.М. Щодо визначення інформаційної безпеки та її різновидів / В.М.Петрик // Форми та методи забезпечення інформаційної безпеки держави : збірник матеріалів міжнародної науково-практичної конференції (м. Київ, 13 березня 2008 р.). – К. : Видавець Захаренко В.О., 2008. – С. 160–164.

7. Информационно-психологическая безопасность в эпоху глобализации : учеб. пособ. / [под. ред. В.В.Остроухова]. – К., 2008. – 544 с.

Грицюк Ю.І.,
доктор технічних наук, професор,
Львівський ДУ БЖД

Хомін Д.М.,
Львівський ДУ БЖД

УПРОВАДЖЕННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ У ДЕРЖАВНІЙ СЛУЖБІ НАДЗВИЧАЙНИХ СИТУАЦІЙ УКРАЇНИ

Зовсім недавно термін “біометрія” широко використовувався в основному коли йшлося про методи математичної статистики, які застосовувалися до будь-яких біологічних об’єктів. Зараз під біометричними технологіями найчастіше розуміють автоматизовані методи розпізнавання особи за біологічними або поведінковими ознаками [2; 3]. Біологічною ознакою може бути будь-який вроджений або повільно змінюваний параметр, індивідуальний для кожної людини. Державна служба надзвичайних ситуацій України (ДСНС України) – одна із державних установ, де тільки в останні роки по-

чали впроваджувати біометричні технології ідентифікації особи. Розглянемо деякі проблеми та перспективи їх упровадження в головних і територіальних управліннях.

Система біометричної ідентифікації особи може зчитати біологічні дані людини та визначити її як особу, зіставивши ці дані з біометричною інформацією в базі даних, отриманою внаслідок попереднього сканування цієї людини. Наразі практичне застосування отримала невелика кількість біометричних показників людини. Найвідомішими є "три великі біометрики", які дають змогу ідентифікувати особистість людини з високою достовірністю розпізнавання [2]: за відбитками пальців – 28,3 %; райдужною оболонкою ока – 26,7 %; зображенням обличчя – 20,8 %. Решта припадає на геометрію руки – 12,5 %, на верифікацію голосу – 9,2 % та підпису – 2,5 %.

Будь-яка система біометричної ідентифікації особи працює за таким узагальненим алгоритмом [3]:

1. Спеціальний сканер зчитує біометричний параметр людини.

2. Шляхом звернення до локальної або зовнішньої бази даних установлюється її особа, тобто отриманий біометричний параметр порівнюється з попередньо зареєстрованим біометричних шаблоном.

3. Приймається конкретне рішення, наприклад, подається команда на відкриття дверей або надається доступ до ПК чи мережі.

Основне призначення будь-якої системи біометричної ідентифікації особи в ДСНС України – позбавлення користувачів проблем, пов'язаних із втратою ключів і посвідчень особи, а також від потреби запам'ятовувати ідентифікаційний код, паролі. Унікальність біометричних параметрів кожної людини робить неможливим їх використання третіми особами [3]. Процес спілкування користувача з біометричним сканером відбувається легко і вимагає мінімальних часових витрат. Процес розпізнавання, завдяки інтуїтивності програмного й апаратного інтерфейсу, зрозумілий і доступний людям будь-якого віку і не знає мовних бар'єрів.

Головне в системі біометричної ідентифікації особи – забезпечення максимальної безпеки і точності ідентифікації. При цьому часто доводиться вибирати між безпекою, точністю і простотою використання. Наприклад, надточна система біометричної ідентифікації особи може бути складною у використанні й не подобатися користувачам через деякі неточності біометричних сканувань. Розчаровані користувачі намагатимуться знайти можливості обійти систему, знижуючи цим самим її ефективність і загальну безпеку [2].

Утім, жодна із систем ідентифікації особи, в т.ч. біометричних, не захищена від неправильного її використання [3]. Кожна біометрична технологія має свої сильні та слабкі сторони. Деякі з цих тех-

нологій є оптимальними для надання доступу до ПК або мережі, тоді як офісні системи можуть використовуватися в багатьох інших середовищах (як зовнішніх, так і внутрішніх).

Стосовно проблеми надійності зберігання біометричних даних. Якщо покупець віддає продавцеві свою кредитну картку або залишає свій відбиток пальця, то він сподівається, що цією інформацією не скористається хто-небудь ще. Проте внутрішня безпека будь-якого підрозділу ДСНС України може бути порушена, а персональні дані, які використовуються для ідентифікації особи, вкрадені [2].

Об'єктом крадіжки може стати навіть уся база біометричних даних, позаяк підрозділи, що застосовують біометричні системи, не застраховані від такої можливості. Якщо у вас вкрали кредитну картку або номер соціального страхування, то ви завжди зможете їх замінити, чого не можна сказати про відбитки пальців. Якщо зловмиснику вдасться замінити в базі даних зображення ваших відбитків пальців, то він зможе отримати доступ до ваших рахунків або конфіденційних документів. Він навіть може спробувати виготовити форму вашого пальця і використовувати її для обману дактилоскопічного сканера.

Утім, компанії – виробники сучасних біометричних систем розробили засоби для обмеження таких ризиків [1]. Розглянемо деякі з них.

Марк Кросбі (Mark Crosbie), головний архітектор із питань безпеки компанії Hewlett-packard, уважає, що багато людей бояться, що їхні відбитки пальців вкрадуть і вони будуть загублені назавжди [2]. Проте, на відміну від паролів, безпека біометричних даних не пов'язана із забезпеченням їх конфіденційності. Компанії, які використовують сучасні біометричні системи, зберігають замість зображень відбитків пальців оброблені форми, так звані шаблони, які є зменшеними цифровими зображеннями відбитків пальців. За допомогою криптографії ці шаблони можна захистити так, що якщо сьогодні їх вкрасти, то вже завтра вони будуть неактуальні. Ступінь захисту бази біометричних шаблонів відбитків пальців, райдужної оболонки ока чи зображення обличчя може бути таким, як і у баз даних номерів кредитних карток або номерів соціального страхування [1].

Наприклад, певний підрозділ ДСНС України бере відбитки пальців, коли працівник реєструється в її системі [3]. Потім зображення перетворюється на 40 унікальних точок на пальці, інформація зберігається в зашифрованій базі даних, а зображення відбитка пальця видаляється. Коли працівник сканує свій палець, біометрична система використовує для його ідентифікації тільки ці унікальні то-

чки. Водночас, самі точки не можуть бути використані для відтворення відбитка пальця працівника.

Використання біометричної технології у поєднанні з паролями і PIN-кодами робить крадіжку особистих ідентифікаційних даних практично неможливою [2]. Проте абсолютно захищеної системи досі не існує. При неправильному використанні біометричні дані й номери кредитних карток однаково не захищені від крадіжки. Надаючи свої біометричні дані, користувачі мають знати ризики їх викрадення та переваги їх використання, оскільки ці системи набувають все більшого поширення не тільки в розвинутих країнах Сходу і Заходу. Скоро вони будуть практично всюди.

Що стосується загальних перспектив розповсюдження та розширення біометричних технологій у структурних підрозділах ДСНС України, то тут аналітики передбачають на найближчі роки зростання кількості охочих їх застосувати приблизно на 25-30 %. При цьому найдинамічніше розвиватимуться відділи ІТ, в основному за рахунок недорогих продуктів для ПК. Однак тут є одна проблема, яка помітно перешкоджатиме масовому поширенню біометричних технологій. Ідеться про захист приватних прав користувачів. Варто згадати хоча б паніку серед користувачів ПК, коли компанія Intel вирішила вбудувати у свої процесори ідентифікаційні номери. У нашому ж випадку відкриваються колосальні можливості для зловмисників щодо збирання персональної інформації про користувачів ПК, та ще й без їх відома!

Загалом проблема надійного зберігання біометричних даних у підрозділах ДСНС України, як і будь-якої конфіденційної інформації, за бажання повністю вирішується [2, 3]. Найскладніше – це переконати людей, що конфіденційність подібних відомостей повністю гарантована. Позаяк, аналітики уважають, що можуть виникнути й певні складнощі суто психологічного характеру: зняття відбитків пальців поки що викликає в багатьох людей певні асоціації з причетністю до кримінальних справ.

Утім, важко не погодитися з тим, що біометричні технології є набагато надійнішими і зручнішими за ті засоби захисту, які широко застосовувалися донедавна, й забезпечують чималі переваги, насамперед, для кінцевих користувачів. Тому багатьом доведеться поступово звикати до думки, що коли-небудь замість пропозиції поставити свій підпис на документі ми почуємо: “Прикладіть руку”. Як свого часу князі, царі та інші повелителі свої укази скріплювали печаткою, яка знаходилася на пальці руки.

ЛІТЕРАТУРА

1. Березин А. Идентификация по радужной оболочке глаза, скорее всего, станет повсеместной нормой, 19 апреля 2012 года / А.Березин. [Электронный ресурс]. – Доступный с http://science.compulenta.ru/674396/.

2. Биометрические средства идентификации личности [Электронный ресурс]. – Доступный с http://xreferat.ru/33/6447-1-biometricheskie-sredstva-identifikacii-lichnosti.html.

3. Биометрия. Изображение лица. [Электронный ресурс]. – Доступный с http:// wiki. oszone.net/index.php/Биометрия._Изображение_лица.

Гулак Г.Н.,
Національна академія Служби безпеки України

ПОНЯТІЙНИЙ АПАРАТ ТА МОДЕЛІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Вивчення виданих у 2011-2012 рр. аналітичних оглядів провідних експертів із питань інформаційної безпеки [1; 2] свідчить про вступ світового суспільства до якісно нової фази протиборства в глобальному інформаційному просторі. Ця фаза характеризується:

– колосальними масштабами проведення атак за географією розповсюдження шкідливих кодів шпигунських програм, а також інтенсивністю фіктивних запитів у випадку проведення DDoS–атак на інформаційні ресурси;

– широким спектром об'єктів атак (здебільшого це автоматизовані системи урядових установ, збройних сил, правоохоронних органів та великих комерційних компаній);

– активними та скоординованими діями порушників, що застосовували кваліфіковано спроектовані засоби нападу.

За різними оцінками, щорічні світові втрати від вандалізму кіберзлочинців становлять від 290 до 750 мільярдів євро.

Необхідність відповіді на виклики сучасності потребує адекватних дій на урядовому рівні, зокрема прийняття необхідних законодавчих актів, розроблення стратегії реалізації організаційних та інженерно-технічних заходів щодо убезпечення не тільки інформаційно-комунікаційних технологій, а й усіх *інтелектуалізованих інфраструктур найважливіших галузей суспільного виробництва та життєдіяльності людини.*